可证安全的无对运算的无证书签密方案 *

陈　虹，赵　悦，肖成龙，肖振久，宋　好

(辽宁工程技术大学 软件学院, 辽宁 葫芦岛 125105)

摘　要：无证书签密体制继承了基于身份签密体制无须使用公钥证书的特点，又对其密钥托管问题进行了改进，具有一定优越性。针对已有的无证书签密方案计算效率低、安全性差等缺点，基于一种安全的签名方案，提出一类新的无对运算的无证书签密方案。采用将哈希函数与用户身份绑定以及公钥与私钥相结合生成新密钥的方法进行构造。在随机预言模型下基于计算椭圆曲线上的离散对数困难问题证明了方案的机密性和不可伪造性。并与已往方案进行对比，在保证安全性的同时，该方案不使用双线性对和指数运算，效率较高。

关键词：无证书签密；机密性；不可伪造性；随机预言模型

中图分类号：TP309.7　　doi: 10.3969/j.issn.1001-3695.2017.10.0938

Certificateless signcryption scheme of verifiable security without pairing

Chen Hong, Zhao Yue, Xiao Chenlong, Xiao Zhenjiu, Song Hao

(*College of Software Liaoning Technical University*, *Huludao Liaoning* 125105, *China*)

Abstract: The certificateless signcryption scheme effectively solved the key escrow problem in identity based signcryption scheme while kept its certificate-free property. Aiming at the low computation efficiency and poor security of the existing certificateless signcryption scheme, this paper proposed a new certificateless signcryption scheme without pairings based on a sort of secure signature scheme. The scheme used binding the hash functions with identities of users and the method of combing the public and private key to generate a new key. The scheme was confidential and unforgeable based on the hard problem of discrete logarithm on the elliptic curve under the random oracle model. Compared with existing schemes, the proposed method improves the efficiency without using bilinear pairing and exponential operation under the secure situation.

Key Words: certificateless signcryption; confidentiality; unforgeability; random oracle model

0　引言

机密性和认证性是密码学中衡量信息是否安全的两个重要指标。为了达到这一标准，传统算法是先将信息进行数字签名，然后加密。但这种方法的计算量是两者之和，效率较低。为解决这个问题，Zheng[1]在 1997 年首次提出签密这一概念。它能在一个逻辑步骤内同时实现签名和加密两项功能，并且与传统算法相比，计算量和通信成本都要更低。此后，签密技术作为热点被广泛研究。

随着签密技术不断发展，基于公钥基础设施（public key infrastructure，PKI）的签密方案被提出，基于 PKI 的签密方案中公钥证书解决了签密方案易受“公钥替换”攻击的问题，通过检验证书的合法性来辨别公钥的正确性。但公钥证书的颁发、验证、管理繁杂和计算量大等问题抑制了该方案的发展。此后，基于身份的签密方案被提出，它取消了公钥证书，避免了证书管理困难等问题。但由于它的私钥完全由私钥生成中心（private key generator，PKG）提供，则出现了密钥托管问题，即 PKG 可以获得任意用户私钥，伪造成任意用户对信息进行解密和验证签名而不被发现，就避免不了会引起安全问题。后来有人又将无证书密码体制与签密体制相结合，形成了无证书签密（certificateless signcryption，CL-SC）体制，它同时解决了基于 PKI 签密方案中的公钥证书问题和基于身份的签密方案中的密钥托管问题。2008 年，首个 CL-SC 方案[2]被提出，后来被验证其不能抵抗扩展不可伪造攻击。随后许多 CL-SC 方案被提出，其中一部分采用了双线性对运算，双线性对运算复杂性高，计算量大。因此，Selvi 等人[3]提出了一个无对运算的 CL-SC 方案，并证明了该方案的安全性。然而在该方案中多次运用指数运算，计算效率依然不高。后来朱辉等人[4]和刘文浩等人[5]也分别提出了无对运算的 CL-SC 方案，但都已被证明是不安全的。

本文在汤永利等人[6]构造的高效、安全的签名方案上，利

基金项目：国家自然科学青年基金项目（61404069）

作者简介：陈虹（1967-），女，辽宁阜新人，副教授，硕士，主要研究方向为网络安全（chh3188@163.com）；赵悦（1992-），女，硕士研究生，主要研究方向为网络安全；肖成龙（1984-），男，副教授，博士，主要研究方向为高层次综合；肖振久（1968-），男，副教授，博士，主要研究方向为网络与信息安全；宋好（1996-），女，本科，主要研究方向为网络安全.

用发送者的私钥与接收者的公钥相结合作为加密密钥，发送者的公钥与接收者的私钥相结合作为解密密钥的方法，构造出一种无对运算的 CL-SC 方案，并在随机预言模型下证明该方案的安全性，与近年的几种签密方案进行对照，其性能更优。

1　预备知识

1.1　数学困难问题

定义在 F_p（F_p 表示有 p 个元素的有限域，p 为素数且 $p>3$）上的椭圆曲线方程为

$$y^2 = x^3 + ax + b \qquad a,b \in F_p$$

判别式为

$$4a^3 + 27b^2 \neq 0 \bmod p$$

椭圆曲线上的所有解与一个无穷远点 O 构成的一个集合用 $E(F_p)$ 来表示，即：$E(F_p)=\{(x,y) \mid x,y \in F_p\}$，且满足方程式 $\{y^2 = x^3 + ax + b\} \cup \{O\}$，$E(F_p)$ 上点的数目用 n 表示，成为椭圆曲线的阶。

椭圆曲线上的离散对数问题：

已知椭圆曲线 $E(F_p)$，阶为 n 的点 $P \in E(F_p)$，$Q \in <P>$，若整数 $x \in [0,n-1]$，使得 $Q=[x]P$。

1.2　CL-SC 方案定义

一个 CL-SC 方案由密钥生成中心（key generation center，KGC），发送者 ID_i，接收者 ID_j 三个合法参与者参与。

一个 CL-SC 方案通常由下列几种算法组成：

a)系统参数建立。由 KGC 运行初始化系统。该算法将安全参数 k 作为输入，KGC 选择主密钥 s，输出系统参数 params。并且由 KGC 保密 s，公开 params。

b)用户部分密钥生成。该算法由 KGC 完成。将某个用户的身份 ID_i、s、params 作为输入，KGC 生成该用户的部分私钥 D_i 和部分公钥 R_i，并返回给用户。

c)用户秘密值生成。该算法由用户独立运行，将 ID_i、params 作为输入，输出一个秘密值 $x_i \in Z_q^*$ 作为长期私钥，并且该值对于 KGC 是保密的。

d)用户私钥生成。该算法由每个用户运行一次。它将 ID_i、D_i、x_i 作为输入，并为该用户生成完整的私钥 $SK_i=(x_i,D_i)$。

e)法用户公钥生成。该算法由用户运行。它将 ID_i、params、R_i 以及 x_i 作为输入，输出用户公钥 $PK_i=(X_i,R_i)$。得到的公钥是公开的。

f)签密(signcrypt)。输入 params、明文消息 m、签密者身份 ID_i 及其私钥 SK_i、接收者身份 ID_j 及其公钥 PK_j，输出密文 σ 并发送给接收方。

g)解签密(unsigncrypt)。输入 params、σ、ID_i、PK_i、ID_j 以及 SK_j，对解签密获得的消息 m 进行验证，如果通过，则用户输出明文消息 m，否则拒收消息 m。

CL-SC 方案组成及通信模型也可由图 1 表示。

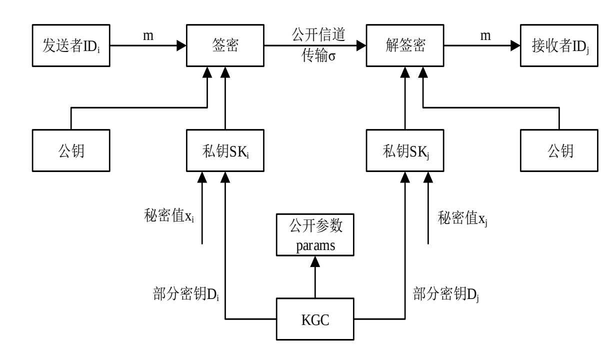


图 1　CL-SC 方案组成及通信模型

发送者 ID_i 利用自己的私钥以及发送者的公钥对明文消息 m 进行签密生成密文 σ，并将密文通过公开信道发送给接收者 ID_j。接收者利用自己的私钥以及发送者的公钥对密文 σ 进行解签密,若所获得的明文能通过验证，则接收。发送者和接收者的私钥都需要一部分由 KGC 提供，一部分为自己生成的秘密值。

2　新的无对运算的 CL-SC 方案

2.1　方案描述

本文构造的无对运算的 CL-SC 方案的具体过程如下：

a)系统参数建立。输入参数 k ,选择一个 l 位的大质数 p，设 G 为椭圆曲线 $E(F_p)$ 的一个循环群，P 为 G 的一个生成元。选择 3 个安全的哈希函数 $H_1:\{0,1\}^* \rightarrow Z_q^*$，$H_2:\{0,1\}^* \rightarrow Z_q^*$，$H_3:Z_q^* \times Z_q^* \rightarrow Z_q^*$。KGC 选择主密钥 s ,并计算主公钥：$P_{pub}=sP$。KGC 保密主密钥 s，公开系统参数 $params=\{p,q,G,P,P_{pub},H_1,H_2,H_3\}$。

b)用户部分密钥生成。给定用户身份 ID_i，KGC 随机选择 $r_i \in Z_q^*$，计算 $R_i=r_iP$，$D_i=r_i+sH_1(ID_i,R_i)$，则生成用户的部分私钥 D_i 和部分公钥 R_i，并将其返回给用户。

c)秘密值生成。随机选择 $x_i \in Z_q^*$ 作为用户的长期私钥。

d)用户私钥生成。生成对应的私钥 (x_i,D_i)。因此，用户 A 的私钥为 $SK_A=(x_A,D_A)$，用户 B 的私钥为 $SK_B=(x_B,D_B)$。

e)用户公钥生成。计算 $X_i=x_iP$，生成公钥 (X_i,R_i)。所以用户 A 的公钥为 PK_A=(X_A,R_A)。用户 B 的公钥为 PK_B=(X_B,R_B)。然后计算等式 $R_i+H_1(ID_i,R_i)P_{pub}=D_iP$ 是否成立。若成立，则 KGC 分配的部分私钥符合规则。

f)签密。当发送者 A 对明文 m 进行签密发送给接收者 B 时，执行以下步骤：

(a)用户 A 随机选取 $t \in Z_q^*$，计算 $T=tP$。

(b)计算 $h_1=H_1(ID_B,R_B)$，$h_2=H_2(m,T,R_A,X_A)$，$u=t+x_Ah_1+D_Ah_2$

(c)计算 $K_1=x_AX_B$，$K_2=(R_B+P_{pub}h_1)D_A$，$V_A=H_3(K_1,K_2)$，加密明文 $c=V_A \oplus m$。

(d)用户 A 向用户 B 发送签密密文 $\sigma=(c,h_2,u)$。

g)解签密。用户 B 收到 $\sigma=(c,h_2,u)$ 后，执行以下步骤：

(a)计算 $h_1^{'}=H_1(ID_A,R_A)$ 和 $T^{'}=uP-X_Ah_1-R_Ah_2-P_{pub}h_1^{'}h_2$。

(b)计算 $V_B=H_3(X_Ax_B,(R_A+P_{pub}h_1^{'})D_B)$，恢复明文 $m=V_B \oplus c$。

(c)计算 $h_2^{'}=(m,T^{'},R_A,X_A)$,若 $h_2^{'}=h_2$，则输出 m，若不成立则拒接。

2.2 正确性证明

新方案的正确性分析如下：

因为

$$\begin{aligned}V_A&=H_3(x_AX_B,(R_B+P_{pub}h_1)D_A)\\&=H_3(x_Ax_BP,(r_B+sh_1)PD_A)\\&=H_3(x_Ax_BP,D_AD_BP)\end{aligned}$$

$$\begin{aligned}V_B&=H_3(X_Ax_B,(R_A+P_{pub}h_1^{'})D_B)\\&=H_3(x_Ax_BP,(r_A+sh_1^{'})PD_B)\\&=H_3(x_Ax_BP,D_AD_BP)\end{aligned}$$

可知，$V_A=V_B$。由于用户 A 通过计算 $c=V_A\oplus m$ 对明文进行加密，用户 B 通过计算 $m=V_B\oplus c$ 对密文进行解密，由于 $V_A=V_B$，所以可以确保用户最后能得到正确的明文。

因为

$$\begin{aligned}T^{'}&=uP-X_Ah_1-R_Ah_2-P_{pub}h_1^{'}h_2\\&=(t+x_Ah_1+D_Ah_2)P-X_Ah_1-R_Ah_2-P_{pub}h_1^{'}h_2\\&=[T+x_Ah_1P+r_Ah_2P+sH_1(ID_A,R_A)h_2P]\\&-X_Ah_1-R_Ah_2-P_{pub}h_1^{'}h_2\\&=T\end{aligned}$$

所以 $h_2^{'}=H_2(m,T^{'},R_A,X_A)=h_2$，说明可以确保解密获得的消息 m 能够通过验证。

3 安全性分析

3.1 安全性定义

判定一个签密方案安全性的基本条件是至少满足机密性即选择密文攻击下加密不可区分性（IND-CCA2）和不可伪造性即选择消息攻击下不可伪造性（EUF-CMA）。根据文献[7]论述，CL-SC 方案通常面对两类攻击者 A_1、A_2 和四类模拟游戏（gameⅠ、gameⅡ、gameⅢ、gameⅣ）。对于第一类攻击者 A_1 而言，不能拥有 KGC 产生的主密钥，但具有替换任意用户公钥的能力。对于第二类攻击者 A_2 而言，它能够获取 KGC 生成的主密钥，则具有构造任意合法用户的部分私钥的能力，但无法替换用户公钥。

文献[8]具体介绍了四类模拟游戏的定义，本文主要以第一类攻击者 A_1 为例，给出在适应性选择密文攻击和选择消息攻击下的示意图，如图 2、3 所示。

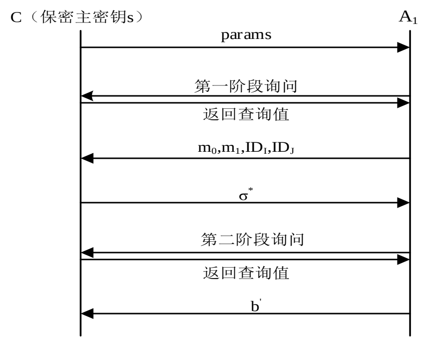


图 2 攻击者为 A_1 的适应性选择密文攻击模拟示意图

其中 C 为该游戏中的挑战者，首先 C 运行系统参数建立算法，将生成的 params 发送给攻击者 A_1，并保密主密钥 s。询问分为两个阶段，第一阶段包括 Hash 函数查询、部分密钥查询、私钥查询、公钥查询、公钥替换查询、签密查询、解签密查询，C 按照要求返回查询值。A_1 选择两个想挑战的用户 (ID_I,ID_J) 和两个等长明文 (m_0,m_1) 发送给 C ,其中未对 ID_J 进行过部分密钥和私钥查询。C 任选其中一明文 m_b $(b\in\{0,1\})$ 进行签密，然后返回密文 σ^* 给 A_1。A_1 进行第二阶段询问，但不可以执行 σ^* 的解签密查询，也不可以执行 ID_J 的部分密钥查询和私钥查询，最后 A_1 返回 $b^{'}$ 给 C。若 $b^{'}=b$，则 A_1 在游戏中获胜。

对于攻击者为 A_2 的适应性选择密文攻击而言，C 运行系统参数建立算法，将生成的 params 和 s 都发送给 A_2。要求在询问阶段不允许进行公钥替换查询，并且在第二阶段的询问中，也不允许对挑战用户进行部分私钥提取查询和对挑战消息进行签密或解签密查询，其他与在 A_1 下攻击过程类似。

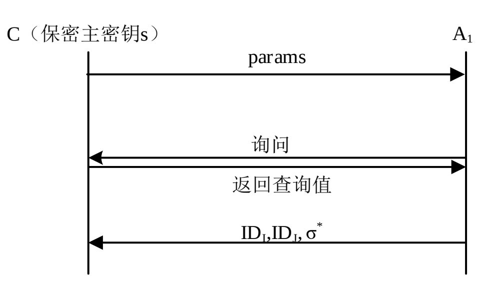


图 3 攻击者为 A_1 的选择消息攻击模拟示意图

挑战者 C 运行系统参数建立算法，将生成的 params 发送给 A_1，并保密 s。A_1 向 C 发起询问，询问阶段与适应性选择密文攻击游戏中第一阶段询问相同。伪造阶段，A_1 向 C 发送元组 (ID_I,ID_J,σ^*)，ID_I 为发送者，ID_J 为接收者，σ^* 为 A_1 从 ID_I 到 ID_J 对明文 m 的签密值，其中在询问阶段未执行过该元组的签密查询，并且也未执行过 ID_J 的部分私钥查询。经过验证，若 σ^* 是对 (ID_I,ID_J,m) 的有效签密，则 A_1 赢得游戏。

对于攻击者为 A_2 的选择消息攻击而言，C 运行系统参数建立算法，将生成的 params 和 s 发送给 A_2。在询问阶段，不进行公钥替换查询，并且在伪造阶段，要求挑战用户未进行过签密查询也未进行过部分私钥提取查询，其他与在 A_1 下的选择消息攻击过程类似。

3.2 机密性分析

若攻击者想从密文 $\sigma=(c,h_2,u)$ 中获得明文，就一定要计算出加密密钥 V_A。若想获得 V_A 则须知道用户 A 的私钥，即使在第二类攻击者 A_2 攻击下，恶意的 KGC 仅有部分私钥 D_A，若想从 X_A 中求出另一部分私钥 x_A，则面临解离散对数问题，从而无法获得加密密钥，无法恢复密文。另一方面，由于 $V_A=V_B$，进而若能计算出 V_B 同样可以破解密文。同理若想求出 V_B 则必须计算出 B 的完整私钥，同样面临解离散对数问题。

该方案的机密性详细证明如下：

引理 1 攻击者 A_1 下的机密性。在随机预言模型且 ECDLP

难解的情况下，在概率多项式时间内存在敌手 A_1 以 ε 的优势赢得游戏 IND-CCA2，则存在一个区分者 C 以 $Succ_{A_1}^{ECDLP} \ge \varepsilon/q_1 \left(1-1/q_1\right)^{q_{pp}} \left(1-1/q_3^2\right)$ 的概率解决 ECDLP 困难问题。

证明 若想攻破本文的 CL-SC 方案，就必须存在算法 C 利用 A_1（第一类攻击者）攻击解决 ECDLP 问题，即已知 (p,ap)，可求 a 的值。

1)初始化 C 运行系统参数建立算法，并保存 s，发送 params 给 A_1。

2)询问阶段

a) H_1 询问：C 维护列表 L_{H_1}，初始为空，格式为 (ID,R_{ID},D_{ID},h_1)，当 C 接收到 A_1 对 $H_1(ID,R_{ID})$ 的询问，若该列表中存在则返回 h_1 给 A_1，若不存在则随机选择 $h_1 \in Z_q^*$ 返回，并加入到列表 L_{H_1} 中。

b) H_2 询问：C 维护列表 L_{H_2}，初始为空，格式为 (m,T,R_{ID},X_{ID},h_2)，当 C 接收到 A_1 对 H_2 的询问时，若该列表中存在则返回 h_2，若不存在则随机选择 $h_2 \in Z_q^*$ 返回给 A_1，并加入到列表 L_{H_2} 中。

c) H_3 询问：C 维护列表 L_{H_3}，初始为空，格式为 (K_1,K_2,h_3)，当 C 接收到 A_1 对 H_3 的询问时，若列表中存在则返回 h_3，若不存在则随机选择 $h_3 \in Z_q^*$ 返回给 A_1，并加入到列表 L_{H_3} 中。

d)部分私钥询问：当 C 接收 A_1 对用户 ID 的部分私钥询问时，若 $ID = ID^*$，则 C 终止；若不等，则查询列表 L_{H_1} 中是否有对应项，若有返回 D_{ID} 给 A_1，若没有则先进行 H_1 询问，再返回。

e)公钥询问：C 维护列表 L_{PK}，初始为空，格式为 (ID,x_{ID},X_{ID})。当 C 接收到 A_1 对某一 ID 的公钥询问时，先进行 L_{H_1} 查询，若存在对应项则返回 R_{ID} 给 A_1；若不存在则先进行 H_1 询问，再返回。C 再查询 L_{PK}，列表中若存在对应项，则返回 X_{ID} 给 A_1，若不存在，则选任意随机数 $x_{ID} \in Z_q^*$，计算 $X_{ID} = x_{ID}P$，再返回 X_{ID} 给 A_1。并把该项加入到列表 L_{PK} 中。

f)公钥替换询问：C 接收到 A_1 关于 $(ID,X_{ID}^{'})$ 的公钥替换询问时，C 查找 L_{PK} 列表，若存在对应项，则用 $X_{ID}^{'}$ 替换 X_{ID} 并令 $x_{ID} = \perp$。

g)私有秘密值询问：当 C 接收到 A_1 对某一 ID 的私有秘密值询问时，C 查询 L_{PK}，若存在相应项且 x_{ID} 有值，则返回该 x_{ID} 给 A_1，若 $x_{ID} = \perp$，则表示公钥已被替换，则 C 返回 $\perp$。

h)签密询问：A_1 选择 (m,ID_a,ID_b) 进行签密询问，其中 ID_a 为发送者，ID_b 为接收者。C 接收到该询问后进行如下处理：若 $ID_a \ne ID^*$ 且 ID_a 公钥未被替换，则 C 通过相关询问并按照签密算法算出密文并返回给 A_1；若 $ID_a = ID^*$ 或 ID_a 的公钥被替换过，则 $ID_b \ne ID^*$，C 查询的 ID_b 部分私钥 D_b 和秘密值 x_b，然后通过公钥查询查出 ID_a 的公钥，再请求 H_3 询问，最后 C 按照签密算法算出密文并返回给 A_1。

i)解签密询问：A_1 作出解签密询问 (ID_a,ID_b,σ) 其中 ID_a 是发送者身份，ID_b 是接收者身份：若 $ID_b \ne ID^*$，则 C 查询表 L_{H_1} 的 (ID_a,R_a,D_a,h_1)、(ID_b,R_b,D_b,h_1)，表 L_{H_2} 的 (m,T,R_a,X_a,h_2) 和 L_{PK} 的 (ID_a,x_a,X_a)、(ID_b,x_b,X_b)，计算 $T^{'} = uP - X_a h_1 - R_a h_2 - P_{pub} h_1^{'} h_2$，计算 V_b，解密消息 $m = V_b \oplus c$，查表 L_{H_2} 中是否存在，若成立则返回 m 否则终止，若 $ID_b = ID^*$ 则终模拟。

当上述模拟结束，A_1 挑选挑战的两个用户身份 (ID_I,ID_J) 和等长的明文 (m_0,m_1) 发送给 C，若 $ID_J \ne ID^*$ 则终止，否则 C 任意选择 $b \in \{0,1\}$，$t^* \in Z_q^*$，计算 $T^* = t^*P$，$h_1 = H_1(ID_J,R_J)$，$h_2^* = H_2(m_b,T^*,R_I,X_I)$，$u^* = t^* + x_I h_1 + D_I h_2^*$，计算 $V_I = H_3(x_I X_J,(R_J + P_{pub}h_1)D_I)$，$c = V_I \oplus m_b$ 最后将 $\sigma^* = (c,h_2^*,u^*)$ 发送给 A_1。

A_1 可以继续询问，但不可以执行 ID^* 的部分私钥和对 σ^* 的解签密查询，最后输出 A_1 对 b 的猜测 $b^{'}$。A_1 若未选择 ID_J 作为挑战用户，进行过 ID^* 部分私钥提取询问，进行过 V_I 的 H_3 询问，则挑战失败。假设 A_1 在多项式时间内至多进行 q_{pp} 次部分私钥询问，q_i 次 H_i 查询。因此 A_1 选择 ID_J 为挑战用户的概率是 $1/q_1$，A_1 未进行过部分私钥查询的概率至少是 $\left(1-1/q_1\right)^{q_{pp}}$，$A_1$ 未进行过 V_I 的 H_3 询问的概率 $\left(1-1/q_3^2\right)$，则 C 成功解决 ECDLP 的概率为 $Succ_{A_1}^{ECDLP} \ge \varepsilon/q_1 \left(1-1/q_1\right)^{q_{pp}} \left(1-1/q_3^2\right)$，证毕。

引理 2 攻击者 A_2 下的机密性。在随机预言模型且 ECDLP 难解的情况下，在概率多项式时间内存在敌手 A_2 以 ε 的优势赢得游戏 IND-CCA2，则存在一个区分者 C 以 $Succ_{A_1}^{ECDLP} \ge \varepsilon/q_1 \left(1-1/q_1\right)^{q_{pp}} \left(1-1/q_3^2\right)$ 的概率解决 ECDLP 困难问题。

证明 若想攻破本文的 CL-SC 方案，就必须存在算法 C 利用 A_2（第二类攻击者）攻击解决 ECDLP 问题，即已知 (p,ap)，可求 a 的值。证明过程与引理 1 相似。

3.3 不可伪造性分析

引理 3 攻击者为 A_1 的不可伪造性。在随机预言模型下且 ECDLP 难解的情况下，在概率多项式时间内存在敌手 A_1 以 ε 的优势赢得游戏 EUF-CMA，则存在一个区分者 C 以 $Succ_{A_1}^{ECDLP} \ge \varepsilon/q_1 \left(1-1/q_1\right)^{q_{pp}}$ 的概率解决 ECDLP 困难问题。

证明 若想攻破本文的 CL-SC 方案，就必须存在算法 C 利用 A_1（第一类攻击者）攻击解决 ECDLP 问题，即已知 (p,ap)，可求 a 的值。

a)初始化。C 运行系统参数建立算法生成 $params = \{p,q,G,P,P_{pub},H_1,H_2,H_3\}$，并将主密钥保存，其他参数发送给 A_1。其中 $P_{pub} = aP$，用 a 模拟系统主秘钥。

b)询问阶段。同引理 1。

c)伪造阶段。当多项式有界询问结束后，A_1 提交用于挑战的两个用户身份 (ID_I,ID_b) 和对某一明文 m 的有效签密 $\sigma = (c,h_2,u)$，若 $ID_I \ne ID^*$ 则终止;否则通过分叉引理[9]，重放 H_2 询问可得两个有效的签密 (c,h_2,u) 和 (c,h_2^*,u^*)。并且 $u^* = t + x_i h_1 + D_i h_2^*$，$u = t + x_i h_1 + D_i h_2$，$D_i = r_i + a \cdot H_1(ID_i,R_i)$，所以可以解得

$a=\frac{(u^{*}-u)/(h^{*}-h)-r}{H_1(ID_I,R_I)}$，进而 C 成功解决了 ECDLP 问题。

若 A_1 对 ID_I 进行过部分私钥询问或 $ID_I \neq ID^{*}$ 则游戏终止。假设 A_1 在多项式时间内至多进行 q_{pp} 次部分私钥询问，q_i 次 H_i 查询。A_1 未对 ID_I 进行私钥询问的概率至少为 $\left(1-{}^{1}\!/_{q_1}\right)^{q_{pp}}$，$A_1$ 选择 $ID_I = ID^{*}$ 作为挑战用户的概率为 ${}^{1}\!/_{q_1}$，则 C 成功解决 ECDLP 的概率为 $Succ_{A_1}^{ECDLP} \geq {}^{\varepsilon}\!/_{q_1}\left(1-{}^{1}\!/_{q_1}\right)^{q_{pp}}$，证毕。

引理 4　攻击者为 A_2 的不可伪造性。在随机预言模型下且 ECDLP 难解的情况下，在概率多项式时间内存在敌手 A_2 以 ε 的优势赢得游戏 EUF-CMA，则存在一个区分者 C 以 $Succ_{A_1}^{ECDLP} \geq {}^{\varepsilon}\!/_{q_1}\left(1-{}^{1}\!/_{q_1}\right)^{q_{pp}}$ 的概率解决 ECDLP 困难问题。

证明　若想攻破本文的 CL-SC 方案，就必须存在算法 C 利用 A_2（第二类攻击者）攻击解决 ECDLP 问题，即已知 (p,ap)，可求 a 的值。证明过程与引理三相似。

4　性能分析

本文提出的新的 CL-SC 方案无须使用双线性对运算和指数运算，在签密阶段使用 6 次点乘运算，分别为 $T=t\cdot P$，$u=t+x_A\cdot h_1+D_A\cdot h_2$，$K_1=x_A\cdot X_B$，$K_2=(R_B+P_{pub}\cdot h_1)\cdot D_A$；在解签密阶段使用 8 次点乘运算，分别为 $T^{'}=u\cdot P-X_A\cdot h_1-R_A\cdot h_2-P_{pub}\cdot h_1^{'}\cdot h_2$，$V_B=H_3(X_A\cdot x_B,(R_A+P_{pub}\cdot h_1^{'})\cdot D_B)$。

下面将从计算效率、正确性、机密性和不可否认性几个方面来对方案进行性能分析。将本文所提出的签密方案与文献[11～14]进行对比，其中分别用 E、P、M 来表示指数运算，双线性对运算和点乘运算。分析结果如表 1 所示。

表 1　签密方案性能比较

方案	签密	解签密	正确性	机密性	不可否认性
文献[11]	2E+6M	2P+2E+5M	√	√	√
文献[12]	2P+5M	2P+5M	√	√	√
文献[13]	1E+2M	6E+7M	√	×	×
文献[14]	5M	5M	×	×	×
本文方案	6M	8M	√	√	√

从表 1 可以看出，文献[11]的方案中使用了双线性对运算、指数运算和点乘运算，文献[12]的方案中使用了双线性对运算和点乘运算。根据 Chen 等人[15]研究表明，执行一次双线性对所消耗的运算量相当于执行 21 次椭圆曲线上的点乘运算。因此，就计算效率方面，本文优于以上两种方案。在安全性上，文献[13]不满足机密性和不可否认性，不能抵抗攻击者 A_1 的公钥替换攻击，即攻击者 A_1 通过替换发送者的公钥，从而冒充发送者伪造签密文发送给接收者而不被发现。文献[14]中的方案在计算签密的过程中使用 KGC 生成的临时秘密值，使整个方案面临主密钥泄露的危险，并且该方案不能抵抗 A_2 的伪造攻击和 A_1 公钥替换的机密性攻击。在文献[16，17]中详细描述对文献[14]的攻击方法，在此不做赘述。因此本文方案比文献[13，14]中的方案更加安全。

5　结束语

本文以汤永利等人的签名方案为基础，构造了一种无对运算的 CL-SC 方案，并在随机预言模型下证明了它的安全性。在与其他方案对比后，可知该方案的性能更优。CL-SC 方案计算开销低、安全性高，在电子支付、无线传感设备、汽车自动驾驶等方面有广泛的应用。然而现有的一些方案仍存在安全性差、效率低等问题，因此如何构造安全高效的方案仍是值得研究的问题。

参考文献：

[1] Zheng Yuliang. Digital signcryption or how to achieve cost (signature&encryption) << cost (signature) +cost (encryption) [C]// Proc of the 17th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 1997: 165-179.

[2] Barbosa M, Farshim P. Certificateless signcryption [C]// Proc of ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2008: 369-372.

[3] Selvi S S D, Vivek S S, Rangan C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction whitout pairing [C]// Proc of the 5th International Conference on Information Security and Cryptology. Berlin: Springer-Verlag, 2010: 75-92.

[4] 朱辉，李晖，王育民. 不使用双线性对的无证书签密方案 [J]. 计算机研究与发展, 2010, 47 (9): 1587-1594.

[5] 刘文浩，许春香. 无双线性配对的无证书签密方案 [J]. 软件学报, 2011, 22 (8): 1918-1926.

[6] 汤永利，王菲菲，闫玺玺，等. 高效可证安全的无证书签名方案 [J]. 计算机工程, 2016, 42 (3): 156-160.

[7] Liu Zhenhua, Hu Yupu, Zhang Xiangsong, et al. Certificateless signcryption scheme in the standard model [J]. Information Sciences, 2010, 180 (1): 452-464.

[8] 沈丽敏，张福泰，孙银霞. 对一种无双线性配对的无证书签密方案的安全性分析 [J]. 密码学报, 2014, 1 (2): 146-154.

[9] Pointcheval D, Stern J. Security arguments for digital signatures and blind signature [J]. Journal of Cryptology, 2000, 13 (3): 361-396.

[10] 周彦伟，杨波，张文政. 不使用双线性映射的无证书签密方案的安全分析及改进 [J]. 计算机学报, 2016, 39 (6): 1257-1266.

[11] 邓伦治，李思维，于亚峰. 高效的无证书签密方案 [J]. 厦门大学学报：自然科学版, 2014, 53 (6): 810-816.

[12] 汤鹏志，张庆兰，杨俊芳. 一种改进的基于双线对的无证书签密方案 [J]. 合肥工业大学学报：自然科学版, 2016, 39 (7): 917-923.

[13] 高键鑫，吴晓平，秦艳琳，等. 无双线性对的无证书安全签密方案 [J].

计算机应用研究, 2014, 31 (4): 1195-1198.
[14] 夏昂，张龙军. 一种新的无双线性对的无证书安全签密方案 [J]. 计算机应用研究, 2014, 31 (2): 532-535.
[15] Chen L, Cheng Z, Smart N P. Identity-based Keyagreement protocols from pairings [J]. International Journal of Information Security, 2007, 6 (4): 213-241.
[16] 郐昌芝. 可证安全的无证书签密方案 [J]. 计算机应用与软件, 2016, 33 (3): 327-333.
[17] 樊爱宛，潘中强，赵伟艇. 两种无证书签密方案的密码分析和改进 [J]. 计算机应用与软件, 2016, 33 (7): 313-317, 333.